UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
SOUTHERN DIVISION
NO. 7:20-CR-0167-3-M

UNITED STATES OF AMERICA	)	
	)	
v.	)	UNITED STATES' RESPONSE
	)	TO MOTION TO SUPPRESS
JORDAN DUNCAN	)	(D.E. 341)
a/k/a "Soldier"	)	

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby responds in opposition to the defendant's motion to suppress electronic data. D.E. 341. For the reasons set forth below, the Court should deny the motion.

BACKGROUND

On August 18, 2021, a Grand Jury charged Defendant with conspiracy to manufacture firearms and to ship firearms interstate without a license, in violation of 18 U.S.C. 371 (Count One) and conspiracy to destroy an energy facility (Count Five). D.E. 149. Count One charges that beginning in or about June 2019, and continuing to the present, Defendant did conspire with others to willfully and knowingly, without a license, engage in the business of manufacturing firearms and in the course of such business to ship, transport, and receive a firearm in interstate commerce. Count Five charges that beginning in or about June 2019, and continuing to the present, Defendant did conspire with others to willfully and knowingly, damage and attempt to damage the property of an energy facility of the United States involved in the transmission and distribution of electricity.

During the investigation, more than a dozen search warrants were executed. They included searches of packages sent by Kryscuk in the United States Mail to others both within and outside

the Eastern District of North Carolina, various warrants to track phone locations, searches of the residences of charged defendants at or near the time of their arrests, specific searches for electronic devices, and searches of social media accounts. The defendant specifically complains of three warrants: an August 20, 2020 warrant issued in the Eastern District of North Carolina for defendant's iCloud account (7:20-MJ-1200-RJ)(D.E. 341 Exhibit A); an October 16, 2020 warrant for defendant's residence and person, to include his cellular telephone, issued in the District of Idaho (1:20-mj-166-CWD)(D.E. 341 Exhibit B); and a follow up warrant issued in the District of Idaho to search the previously seized property for crimes of a different nature (1:21-mj-410-CWD)(D.E. 341 Exhibit C). The three warrants authorized seizure of the account, devices, and material at issue, and provided for a targeted search as specified. D.E. 341, Exhibit A at 7 – 8 (Bates numbered B002645-46), Exhibit B at 41 – 45 (Bates numbered A011567 -72), and Exhibit C at 55 – 59 (Bates numbered A011672 – 76). The law is clear and against the defendant's claim for relief; obtaining the entirety of the account, device, or material and executing an approved, targeted search is lawful under the Fourth Amendment.

ARGUMENT

The defendant argues these three warrants fail the particularity requirement and amounted to unlawful general warrants. D.E. 341 at 7. "Federal courts, however, have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers, because 'criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity [such that] a broad, expansive search of the [computer] may be required.'" United States v. Bass, 785 F.3d 1043, 1049–50 (6th Cir. 2015) (quoting United States v. Stabile, 633 F.3d 219, 237 (3d Cir.2011) and citing United States v. Richards, 659 F.3d 527, 539 (6th Cir.2011).

The Fourth Amendment requires that every warrant "particularly describ[e]" not only "the place to be searched," but also "the persons or things to be seized." U.S. Const. Amend. IV; see United States v. Grubbs, 547 U.S. 90, 97 (2006). When search warrants authorize the seizure and examination of computers, it is true these "particularity" requirements take on special importance. "The ability of computers 'to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.'" United States v. Burke, 633 F.3d 984, 992 (10th Cir. 2011) (quoting United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)). See also, Riley v. California, 573 U.S. 373 (2014).

Nevertheless,

> if there is probable cause to search a computer for evidence of a crime, that probable cause is usually sufficient to sustain a search of the entire computer. A search of a cell phone is analogous to a search of a computer. And a search of a computer is analogous to a search of a large file cabinet. Thus, for purposes of the Fourth Amendment, a cell phone can be conceptualized as an enormous filing cabinet.
>
> As one district court in this circuit recently noted, our Court of Appeals has twice rejected the paradigm that would require, in the context of searches of electronic devices, warrants to describe the manner of the search or constrain it to items already known to law enforcement. While the Fourth Amendment might require more specificity as to the place to be searched or the items to be seized in some computer searches, officers are generally not required to predict the items of evidence that an electronic search will uncover or predict where on the computer the evidence will be found.

United States v. Bolling, No. CR 2:21-00087, 2023 WL 5616188 at *6 (S.D.W. Va. Aug. 30, 2023) (internal citations and quotations omitted, but generally see Riley v. California, 573 U.S. 373, 393, (2014); United States v. Cobb, 970 F.3d 319, 329 (4th Cir. 2020), as amended (Aug. 17, 2020), cert. denied, 141 S.Ct. 1750 (2021); United States v. Williams, 592 F.3d 511, 520 (4th Cir.

2010), cert. denied 562 U.S. 1044 (2010); United States v. Bishop, 910 F.3d 335, 337 (7th Cir. 2018); United States v. Skinner, No. 3:19CR19, 2021 WL 1725543 at *15 (E.D. Va. Apr. 29, 2021).

The defendant cites the concurring opinion in a Ninth Circuit case for the proposition that ex ante search protocols need be a part of every warrant authorized. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc). In 2009, the Ninth Circuit announced sweeping new rules for warrants to search computers. The case involved four separate opinions from Ninth Circuit panels; the latter two were en banc. The facts of Comprehensive Drug Testing case involved a criminal investigation, but the case itself was a dispute between the United States and parties not charged with the violation of criminal law. Investigating the illegal distribution of steroids, the United States received search warrants that would allow it to search a private drug testing firm for the test results of ten named baseball players. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 993 (9th Cir. 2009), withdrawn and superseded, 621 F.3d 1162 (9th Cir. 2010) (en banc). In executing one of those warrants, the agent copied a file directory off of a network server. Id. at 993, 1016. The file directory included, among hundreds of other documents, an Excel spreadsheet that contained the names of baseball players who had tested positive for steroids. Id. at 1016. The agents took an electronic copy of the entire directory off-site for later review. The drug testing laboratories moved for a return of their property; district courts granted those motions; and the United States appealed. Id. at 997.

The Ninth Circuit's now-superseded 2009 en banc majority opinion departed from the issues before it and described how magistrates and the government "should" act in the future. Id. at 998. Among several other requirements, it wrote that:

> in "future" applications, the government "should ... forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it

> has gained access only because it was required to segregate seizable from non-seizable data." Id. In requiring the government to "forswear" plain view, the court did not hold that the plain view doctrine does not apply to computer searches; to the contrary, the court described plain view as a "doctrine that would allow [the government] to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data;" it merely advised magistrates to demand a "waiver" or "forswear[ing]" of plain view.

Id. The opinion also held that the warrant should include a written protocol preventing "agents involved in the investigation" from examining or retaining "any data other than that for which probable cause is shown." Id. at 1000. Repeating that instruction, the court rephrased it by saying that only "information for which [the government] has probable cause" may be "examined by the case agents." Id. at 1006.

However, a little more than a year later, the Ninth Circuit superseded its own en banc opinion, replacing it with a per curiam opinion that omitted the new procedural steps the prior opinion had endorsed. See Comprehensive Drug Testing, Inc., 621 F.3d at 1165. Notably, the revised en banc majority opinion omitted all the new procedures announced by the prior opinion. Those procedures were described only in a concurring opinion joined by five of the eleven judges on the en banc panel. Id. at 1178-80. Two circuits, the Third and the Seventh, have explicitly rejected the Ninth Circuit opinion. See Stabile, 633 F.3d at 241 n.16 (3d Cir. 2011) and United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010). As noted in the opinion issued in the last 60 days in Bolling, the Fourth Circuit "has twice rejected the paradigm that would require, in the context of searches of electronic devices, warrants to describe the manner of the search or constrain it to items already known to law enforcement." Bolling, No. CR 2:21-00087, 2023 WL 5616188 at *6. "Insisting that warrants carve out portions of computers and cell phones to be searched (thereby making other portions of the devices completely off-limits to law enforcement) has surface appeal but is neither constitutionally required nor practical in most circumstances. As

courts have had to recognize, the nature of electronic evidence requires that filtering occur at the review level. This means that a cursory review of innocuous material may sometimes happen in order to establish what information is relevant." Id. (internal quotations and citations omitted).

The Tenth Circuit cases cited by the defendant were discussing situations where there was literally no description or limit of what could be seized or which held the opposite of what is implied. D.E. 341 at 10. See, for instance, the Burgess holding. Defendant cited Burgess as saying "If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement.' D.E. 341 a 10. While technically true, that quote is immediately followed by these two sentences: "But a word is known by the company it keeps. The search, in general, was limited to evidence of drugs and drug trafficking and, as it relates to the computer, was limited to the kind of drug and drug trafficking information likely to be found on a computer . . ." United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009)(internal quotation and citation omitted). The Tenth Circuit Court actually went on to hold "[w]hile officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, a computer search may be as extensive as reasonably required to locate the items described in the warrant based on probable cause. And this Court has never required warrants to contain a particularized computer search strategy. The warrant here did not direct the search by describing file name extensions (.doc, . wpd, .txt, .jpg, .gif, etc.), file names or directory structure. Rather the limitation on the scope of this search was explicitly constrained by content—computer files containing evidence of drug use or trafficking." Burgess, 576 F.3d at 1092-93.

In the instant case, the first two warrants sought evidence of violations of 18 U.S.C. § 922(a)(5) and 26 U.S.C. §§ 5801-72.[1] The affidavits set forth a substantial basis to believe such evidence existed in Duncan's account and on his device(s). The warrant authorized the search for any records and items which included communication, indicia of use, ownership, or possession, address books, e-mails, and chat logs *specifically related to the named violations of law*. See D.E. 341, Exhibit A at 7 – 8 (Bates numbered B002645-46), Exhibit B at 41 – 45 (Bates numbered A011567 -72), and Exhibit C at 55 – 59 (Bates numbered A011672 – 76). At the time of the seizure of the account, device or material, however, the agents could not have known exactly where this information was located in the account or device(s) or in what format. Thus, the scope of the warrants were reasonable under the circumstances at that time, of sufficient particularity, and not "general" warrants in violation of the Fourth Amendment..

Assuming arguendo the warrants are defective for any reason, the Leon good faith exception applies and suppression of the evidence is not warranted. The good faith exception requires the government show only that the agent's reliance on the warrant was not unreasonable. "This is a less demanding showing than the 'substantial basis' threshold required to prove the existence of probable cause in the first place." United States v. Bynum, 293 F.3d 192, 195 (4th Cir. 2002). "Courts suppress evidence that is obtained in violation of binding precedent because responsible law enforcement officers will take care to learn what is required of them ... and will conform their conduct to these rules. But applying the Fourth Amendment to social media

[1] The third warrant actually indicates the careful nature in which the agents reviewed the devices - it is a follow up warrant after evidence was discovered in plain view that pertained to a potential violation of a different statute than that contained in either of the first two search warrants. Rather than proceeding with the search through those devices, the search was halted and further, more broad search authority was obtained. See D.E. 341, Exhibit C at 21 – 29 (Bates numbered A0011638 – 45).

accounts is a relatively unexplored area of law with nuances that have yet to be discovered. Courts should not punish law enforcement officers who are on the frontiers of new technology simply because they are at the beginning of a learning curve and have not yet been apprised of the preferences of courts on novel questions." United States v. Chavez, 423 F.Supp.3d 194, 208 (2019) (internal quotations and citations omitted). See also United States v. Cawthorn, No. CR JKB-19-0036, 2023 WL 3735587 at *2 (D. Md. May 31, 2023).

CONCLUSION

For the above-stated reasons and in accord with the applicable law, the defendant's motion to suppress the evidence obtained from searches pursuant to the three contested warrants (D.E. 341) should be denied.

Respectfully submitted, this 9th day of October, 2023.

MICHAEL F. EASLEY, JR.
United States Attorney

By: */s/ Barbara D. Kocher*
BARBARA D. KOCHER
GABRIEL J. DIAZ
Assistant U.S. Attorney
150 Fayetteville St., Suite 2100
Raleigh, NC 27601
Telephone: 919-856-4530
Fax: 919-856-4487
E-mail: barb.kocher@usdoj.gov
NC Bar: 16360
E-mail: gabriel.diaz@usdoj.gov
NC Bar: 49159

CERTIFICATE OF SERVICE

This is to certify that I have this 9th day of October 2023, served a copy of the foregoing filing upon counsel for the defendant in this action by electronically filing the same with the Clerk of Court, using the CM/ECF system that will send notification of such filing to counsel for the defendant, Raymond Tarlton.

/s/ Barbara D. Kocher
BARBARA D. KOCHER
Assistant U.S. Attorney
150 Fayetteville St., Suite 2100
Raleigh, NC 27601